# The various regulatory techniques on the Internet and the role of state law

Poullet, Yves

*Published in:*
Economia e diritto del terziaro

*Publication date:*
2001

*Document Version*
Publisher's PDF, also known as Version of record

# The various regulatory techniques on the internet and the role of state law*

**di Yves Poullet**

*1. Positioning the problem* – As we have seen (n. 13), technology can serve to regulate behaviour on the information superhighway. There are others with which the law may even maintain a dialogue.

The first part will identify the different regulatory techniques applicable to the Internet or generally to information superhighways; the second will analyse the various responses in state and supranational law to these different regulatory techniques and envisages some criteria to enable the legitimization of non-state regulatory systems.

## A. On the diversity of regulatory models

*2. Preliminary considerations* – The goal of regulation is the prescription of behavioural norms. That said, the diversity of regulatory models and the application of norms can be divided according to four criteria: the object, the author, the subject and the sanction *of the norm.*

We may note at the outset that the international dimension of the Internet leads to a certain competition between the different national regulations. As soon as one country decides to regulate certain activities, the parties concerned by the legislation are free to move their activities to another country with a more flexible and less strict regulatory framework. This phenomenon of "regulatory dumping" is real

* The paper has been written in March 2000 in the context of the E.U. Commissioned ECLIP Project. On this project, have a look at the website: http://www.eclip.org.

(Poullet, Queck, 1997). On the other hand, advantages can accrue to the consumer who prefers the security that is granted by a regulatory environment that takes better care of his interests. This second aspect should not be neglected.

*3. An enumeration* – It is impossible to number all the many normative sources of law on the Internet. To those public sources of law, the national state and international norms, are contrasted the private, based either on contractual liberty, or on that which tends to be called self-regulatory, of which one can distinguish aspects of certification and usage that some see as an emerging "lex electronica" parallel to "lex mercatoria" but developed within an electronic context. The technology itself may equally have a normative effect on behaviour.

As regards these private sources, we may observe that the actors themselves have developed means to assure that the self-regulatory code passes from the letter to the act. Thus the co-ordinators nominated within discussion groups are expected to vet incoming messages. The sanctions typical to the network, such as disconnection and "flaming" remind one strangely of vigilante justice. The hot lines created within the framework of certain codes of conduct to enable the denunciation of activities contrary to that code, represent another example of the means set up to assure adherence to network discipline. More interesting still are the labelling and rating mechanisms developed by certain servers which both guarantee and inform the user of the quality of the service being offered (such as the "privacy friendly" label or the one as regards web sites of journalistic informations referring to respect for the press code). Evidently, the value of such a classification depends on the certifying body that defined, issued and controlled it. It is appropriate to mention the North American initiatives for the creation of "virtual magistrates", on-line arbitrators or mediators who are authorized to adjudicate conflicts arising out of network use, whether they be issues of defamation, intrusion into the private sphere or non-respect of the rules of a news group. These alternative Dispute Resolution mechanisms have been recently promoted by the European directive on certain legal aspects of Electronic Commerce in the internal Market.

Briefly, we can see that private regulatory sources set up their own mechanisms for expressing the rules, controlling their application and finally for sanctioning non-respect sanctions pronounced by their own "magistrates". The following reflections will develop certain summarizing remarks concerning the various private and public regulatory sources.



*a) State norms*

*4. With regard to state norms* – That the nation state constitutes a legitimate authority for Internet regulation is clear.

The modalities for the development of the norm are meticulously described in the texts and procedures surrounding this development, thereby guaranteeing a democratic discussion. Application of the norm is granted to "professional" jurisdictions, surrounded by guarantees of independance and adversarial principles.

With regard to "electronic environments" (Trudel, 1997), we can observe two distinct tendencies in state law. The one is a preference for notions of variable content, called standards, and the other the entrusting of the interpretation of these standards to relay bodies, sometimes qualified as independant administrative authorities. If we take the belgian model as a simple example so far the other western european countries have similar institutions, we underline the creation of multiple institutions, notally, as regards the privacy questions: the Privacy Protection Commission (Commission de Protection de la vie privée), as regards the regulation of the audiovisual sector: the Higher Audiovisual Council (Conseil Superieur de l'Audiovisuel) or the Media Council (Mediaraad), as regards the telecommunications sector: the Belgian Institute of Post and Telecommunications (I' Institut Belge des Postes et Telecommunications) (Poullet, 1993).

The international dimension of information superhighways leads states to search, at the international level, for models for developing the law, or for co-operation among the national authorities entrusted with the application of national laws (Frydman, 1997). Whether through international conventions such as those of the I.T.U., W.T.O., W.I.P.O., O.E.C.D, bodies such as the G7, whether it is at the level of treaties of police co-operation amongst those engaged in the fight against cybercrime (cf. the draft Council of European convention about cybercrime), a number of public initiatives have been taken to maintain the role of the state in the protection and safeguarding both of individual rights and of the overiding public interest. Some (Lavenue, 1996) go so far as to suggest the creation of an "International Cyberspace Authority", as a reaction to movements for the emancipation of Internet law and in the face of the increasing power of private norms, this is a question we shall now broach. The "Global Business Dialog" promoted by the European Commissionar: M. Bangemann stresses the importance of setting up this global authority and fixing global rules for the electronic commerce.

*b) Private norms*

*5. Regarding contracts* – The interactivity of networks gives the consent of the internet's user unprecedented implications. Whether to say yes or no to a cookie, to agree to a particular process, to reveal his identity or not, to object to non-solicited correspondence,... whatever the issue, technology renders the internaut responsible for his or her actions (Dunne, 1994; Trudel, 1996). Tempted by the contractual paradigm inherent in the Internet environment, some authors consider that the responsibility of the state to regulate behaviour has been usurped by the sustitute responsibility of the citizen, who by his or her consent chooses to authorize, or not, this or that operation.

The principles of autonomous will and the contract law, unanimously recognized in every jurisprudence, give this approach, founded as it is on the responsibility of the individual Internaut, considerable weight. The contractual approach evidently requires that the technology permits such choices, hence the questions: does the Internaut wish to be identified? for what finalities? within which time limit? must be the object of on-screen choice pages and the system's configuration must guarantee the respect of such choices.

*6. Regarding self-regulation* – Trudel (1989) defines self-regulation as "norms voluntarily developed and accepted by those who take part in an activity". We are familiar with the proliferation of such codes, sometimes drawn up locally in a university or in a newsgroup, sometimes on a larger scale for a direct marketing sector or even for the broad mass of activities on the net (National charters). The Internet Society, a purely private organization entrusted with assuring the international co-operation and co-ordination in technology and programming for the Internet, publishes directive guidelines for Internet and network use. Its president, V. Cerf, affirms as follows: "It is no longer adequate to base guidelines for conduct purely on the basis of who pays for the underiying network or computer systems resources. Even if that was once sensible, the diversity of constituents of the Internet makes it a poor basis for formulating policy. Thus guidelines for conduct have to be constructed and motivated in part on the basis of self-interest. Many of the suggestions below are based on the theory that enlightened self-interest can informa and influence choices of behaviour" (V. Cerf, 1994).

The justification for this galloping self-regulation is a triple one. The argument concerning the technical and evolutionary nature of the object that this self-regulation is designed to cope with is joined by



the argument that only the authors themselves are capable of perceiving the risks involved in particular solutions or, more important still, of assessing the adequacy and effectiveness of sanctions. The immediate blocade by access providers of a site that has been denounced via a hot line mechanism constitutes a more appropriate and effective response to a pomographic site than any judicial condemnation (Hardy, 1994). The possibility of their development and expansion at a world level serves as a supplementary argument, at a time when the global dimension of cyberhighway problems is uncontested.

Beyond the establishment of norms, self-regulation claims to offer models for applying these norms in virtual communities, as distinct from spatial communities localized in a given territory and subject to state legislation. For a while now we have been aware of the role of played by network "moderators", of the first experiences of "cyber-magistrates", of virtual tribunals charged with resolving litigious issues in the virtual world. The creation of councils charged with the application of Internet charters represents another demonstration of self-regulation's aptitude, not only to develop a supple system of law for cyberspace, but also to sanction it (Perritt 1993, Dunne, 1994). There is considerable temptation to see self-regulation as more than just a source of law complementary to that of the state, but rather as a replacement for the latter (Johnson-Post, 1996) or in any case to dispense the State from a meddler regulation. So, in certain cases, the private norm will take the place of a legislation: for example, the manner in which the delicate question of the attribution of Internet's domain-names is currently dealt with certainly argues a good case for the integrity and sufficiency of self-regulatory solutions (Wilkinson, 1998). In other cases, and the present debate between the U.S. administration and the E-U authorities about the Safe Harbour privacy principles is a good example, the code of conduct or the private norm, even this self regulation solution is promoted even requested by the public authorities, will permit these last ones not to set up an intricate and complex administrative and regulatory system which is considered as not useful beyond the vague legal principles already recognized by the Courts. (B. Gellmann, 1998).

*7. As regards certification* – In a global environment where the network represents the sole means of communication, the development of certification as a procedure by which a third party guarantees the specific quality of a person or product seems a happy solution (Courbet et alii, 1995).

The aim of certification is to assure the Internmaut firstly of the existence and address of his interlocutor, secondly of the other's pro-

fessional status (cfr. supra, the electronic signature). Beyond this, questions of conformity of the others products to this or that norm arise, of his processes to this or that privacy legislation, or of his practices to required consumer protection standards or legislations and, finally, the issue of the general security of sites. So many problems which can be the object either of specific certificates (as, for example, the label delivered by the Internet Consumer Protection Agency (ICPA) or by Trust-e which deals only with questions of conformity to privacy standards) or of certification of a more global nature (such as the "Webtrust" initiative developed by the Association of American Accountants).

Certification presents a solution which may be complementary either to a state normative source, or to self-regulation, inasmuch as it refers either to a law, or to a code of good conduct. Essentially it is simultaneously based, on the one hand, on the quality of the certifying authority and their verification procedures (independance, expertise) and, on the other hand, on the effective responsibility of these authorities in the event of the unwarranted issue of a certificate. Finally, certification permits easy and effective sanctioning, inasmuch as the company or individual fears the loss of certification and the negative publicity that this would entail (Poullet-Royen, 1998).

*8. As regards "best practices" and the so called "lex electronica"* – Beyond the codified and well identified sources we have referred to so far, we must also deal with principles, either more diffuse or not, which are to be found in the "Acceptable Use Policies" suggested by Internet access providers, the servers. This "Netiquette" is a sort of "Ten commandments" or a highway code defining the fundamental rules for Internet surfers (Rinaldi, 1995).

These are as follows:

1. You shall not use a computer to harm another person
2. You shall not interfere with another's work
3. You shall not feret about in another's files
4. You shall not use a computer to steal
5. You shall not use a computer to bear false witness
6. You shall not use or copy a program for which you have not paid
7. You shall not use the resources of another's computer without authorization
8. You shall not misappropriate another's intellectual creation
9. You shall envisage the social consequences of the program you are writing
10. You shall use the computer in a manner which shows consideration and respect

As regards the contravention of these rules, we may observe that sanctions can take the form of an organized reaction or not: "flaming", the disconnection of an indelicate user, the threat of contacting the police etc. (North, 1997).

The comparison between such "best practices", spontaneously developed by virtual communities, and the rules of conduct habitually practiced by trading communities, leads one to consider "lex electronica" as close to "lex mercatoria" (Wittes, 1995). The similarity is all the more seductive even if some authors (Frydman, 1997; J.N. Brouir, 1996) denounce the dominant economic debate as one which would "lead to the submission of the information society in general, and the activities of the Internet in particular, solely to the laws of the international marketplace".

This parallel tends to lend authority to the reflections which now follow on the role of state law in the face of diverse regulatory techniques.

## B. The role of state legislation in the reception and promotion of "private" sources of cyberspace law

*9. Preliminary reflections – the necessity of dialogue* – P. Trudel (Trudel, 1997), paraphrasing an observation from H.H. Perritt (Perritt, 1992), wrote: the parties engaged in international transactions, for example, have developed law-creating practices. Interesting parallels can be drawn here with regard to the regulation of electronic-commercial environments, even though we cannot currently speak of the emergence of a genuine corpus of generally applicable rules. The future of this process of normalisation will be favourized by the development of more general practices of international arbitration, carried through without regard to differing national legislations. Even if the customs and practices of a given field of activity are often taken into account and, to a certain degree, integrated into state legislation, the nub of such a norm still rests in its capacity to autonomously organize behaviour and transactions among the members of a community. Respect of these customs and practices is, under certain circumstances, an essential prerequisite for a participant's admission to a given community. Certainly, if the importance of the community justifies it, these customs and practices can constitute a complete regulatory technique, parallel to state legislation, regulating the relationshi-

ps of members of a community and administered by their own authorities. The model of lex mercatoria from the middle ages is frequently cited as an example. Several current debates are involved with the opportunity of developing a similar juridic framework for the regulation of cyberspace; this issue will be analysed here".

This doctrinal reflection on lex mercatoria has led a number of authors (Rigaux, 1977; Santi Romano, 1975) to see in it the opportunity for a clear and indiscutable recognition of our essential normative pluralism. Developing this idea, Rigaux (1977) writes: "the citizen of a state may possess goods in, or reside in, another state, adhere to an organized religious confession, be a member of a transnational professional organization. The law of each of the states to which he is subject, the law of the church to which he is affiliated, the contractual engagements to which he subscribes in the exercise of his individual economic rights, these all present a variety of distinct juridic authorities, each one but imperfectly suited to the others".

In this perspective, self-regulatory texts and, more generally, those private sources of legislation that some choose to refer to as "soft" law, seem in fact to be legal systems in the full sense of the term, even though their creation may seem less legitimate than the more traditional public process of enactment, followed before the final adoption of an Act.

In other respects, without being naïve, we must realize that such a system of regulation by the parties themselves is far from being gratuitous. Operators are concerned by such measures either to side step national legislations or to subject them to a "soft" interpretation, yet notably avoid the levying of grave accusations. The debate on pornography via the Internet, arising from certain recent events, and the resultant proliferation of self-regulatory measures in this respect, well illustrates the argument.

### *a. The "reception" given private sources by state law*

*10. The three law: contact fair trade and responsibility* – The general and universal principles of state law, particularly those of contractual autonomy, fair and equitable trade and responsibility can be taken initially as a control model for private sources of "Cyberlaw".

In that context, one has to underline the different targets pursued by the authors of a code of conduct. Traditionnally, the sole target of the self-regulation was to fix the rules of behaviours between the actors, authors or represented in the process of settling-up the code of conduct. the main aim is then to avoid unfair and wild competition between them. Sometimes, the code of conduct will pursue another goal and provide solution with external effects outside the circle of the natural adressees of the code that is to say the authors or the representatives of the actors concerned by it. So, when the self-regulation defines the acceptable professional behaviours vis à vis third parties concerned by the operations regulated by the code of conduct, it is quite clear that the code of conduct intends to have effects vis à vis third parties including especially but not only parties contracting with the actors submitted to the code of conduct. To take an example, if a Direct marketing Association forbids or at the contrary accepts certain advertising methods or messages, this attitude might affect the third parties independantly of the fact that they will become contractual parties. This external effect of the code of conduct is at the legal point of view more questionable than the internal effects.

As regards the external opposability of the code of conduct to persons which are not only third parties but which will become contracting parties and in that quality, will be considered as submitted to the content of the code of conduct, it would doubtless be sufficient for a judge to go "to the limits of contractual logic", as Vivant (1997) assures us, to become aware of the absence of fully free and informed consent on the part of the internaut in accepting a "policy" or a code of conduct that barely respects his interests. This approach will put into question not only the content of the private norm, its conformity with the legal rules, its clarity, its possible unfair character but also, the integration of the code of conduct within the scope of the contract, which might be questionable when the code of conduct is referred only by an hyperlink uneasy to activate.

As regards the other "third parties", which might consider to be prejudiciated by a behaviour although in strict conformity with the content of the code, the recourse to standards such as " good faith", "bonus pater familias"; those " as well as possible" forms often permit lip service to the adoption of an ethical code, respectful of its norms of prudence and diligence and its sanctioning of violations of a norm developed by a private judicial system, to the degree in which that norm represents a professional standard whose contravention automatically constitutes a fault (F. Osman, 1995). On the contrary, recourse to standards authorizes the denunciation of self-regulation or systems of certification whose content does not seem to respect such standards.

Finally, within a sector, the adoption by one faction of "codes of conduct" or of "technical norms" may be intended to prejudice the competition in some way. It will be sufficient to invoke the principles of free and fair trade to strip them of all value.

*11. Rejection of private legal systems where public order has been contravened* – The body of jurisprudence dealing with the activities of associative authorities, both at the time of the enactment of disciplinary rules and during their application, permits us to extrapolate certain rules which are relevant when tackling the subject of selfregulation, in cyberspace. The applies equally to legal systems whose right to create norms is undisputed. Case law has sometimes, while not contesting the autonomy of the norms enacted by a given profession nonetheless called them into question, particularly in the following situations (N. Decoopman, 1989).

- when the norm is in conflict with a state norm judged to be in the public interest. Thus a code of conduct authorizing a server to process data obtained by means of cookies, without prior information of the internaut concerned would constitute an infringement of the principle of transparency upheld by the data protection directive. Furthermore, the space available for self-regulation is reduced each time a conflict involves a fundamental value. State law will either by decree or recognition proclaim such norms as being in the public interest. This assertion should, however, be nuanced by the following consideration. The effectiveness of the state norm can be reduced insofar as the state authority does not possess the means to enforce it. In such a hypothesis, the state recognized norm is granted a value more symbolic than real, and self-regulation may represent the lesser evil;
- when the application of the norm represents an abuse of rights inasmuch as the sanction is disproportionate to the infraction concerned, or its levying has not taken into account the minimum right to defense according with the article 6 of the European Human Rights Convention. This question is delicate so far the selfregulation pretends to external effects particularly when privacy or consumer protection questions are adressed by the code of conduct or by technical norms. One would like to underline the very interesting solution foreseen by the article 17 of the Directive on certain legal aspects of the electronic commerce: "Member States shall ensure that that bodies responsible for out of court settlements of consumers apply the principles of independance and transparency, the adversarial principle, and the principles of effectiveness of the procedure, legality of the decisions, liberty of parties and representation".

In an Internet context there are certainly instances of sanctions which, through their unilateral application by less than transparent authorities without any external control, may be deemed abusive of a party's rights. Thus the immediate revoking of a website owner's certificate for alleged behaviour of non-conformity to a code of conduct may appear as unacceptable censorship by a judge or by a state authority concerned with the respect of freedom of expression and the adversarial principle.



### *b. The promotion of the private legal systems: reflections on the 95/46 data protection directive*

*12. Two types of promotion* – Taking as a departure two provisions of the directive referred to, we should like to show:

- with reference to Article 27, how state law articulates both public and private norms and thereby promotes the adoption of the latter;
- with reference to Article 25, how a national juridic authority, while respecting the culture and system of other juridic authorities, can establish certain criteria for the recognition of private norms conceived in those other juridic authorities.

*13. "Monitored codes of conduct"* – Article 27 § 1 of the directive asserts that the E.U. member states "encourage" the enunciation of codes of conduct destined to contribute, depending on the specific nature of the sectors concerned, to the correct application of national provisions. The editors of such codes could submit them to the national Data Protection authorities which would verify their conformity with existing regulations.

The text also envisages the drawing up of community codes which could be submitted to the European Data Protection Working Group which would examine their respect of national provisions.

Once the codes have been submitted for their inspection, both the national authority and the European Working Group could, "should they deem it appropriate", gather the opinions of the persons concerned or their representatives. Finally, depending on whether the code was national or European, each of these authorities respectively could take steps to ensure publication (Boulanger et alii, 1997).

The directive's principle is a simple one: taken downstream of the principles of the directive, both self-regulation and certification represent effective tools for the their enactment. They contribute to the improvement of the brand image of those who submit to them and increase the confidence of the internaut. Their flexibility and specificity

make them suitable tasks for evolutive solutions adapted to the particularities of each sector. Finally, their European character serves to guarantee the equivalence of protection with regard to electronic processes operating in any corner of the continent.

Recognition by state authorities of these codes of conduct takes two forms.

- the formal procedure of confirmation does not only apply to the basic criteria which constitute respect for the provisions of the directive, but also to more procedural criteria: the publishing of the content of selfregulation or criteria for certification, the transparency and openness of debates, taking into account the range of parties interested in these processes, in particular those directly concerned;
- in any event, the codes of good conduct cannot exempt the server from applicable areas of national legislation derived from the directive which guarantee, admittedly in general terms, the respect of subjective rights and the possibility of appeal to justice for the persons concerned. Such submission to the law brings to codes of otherwise restricted range, if only indirectly, a certain legal weight, given the fact that the law, accompanied by the restraining force of justice, remains the ultimate guarantee of the effectiveness of the principles enunciated therein.

The European Council Recommandation dated from the 24 th of september 98 ( 98/560/CE) "about the development of the competition within the audiovisual and information services by promoting the protection of minors and human dignity" is going further. A number of indicative guidelines are annexed to the recommandation. These guidelines are aimed to ensure a full participation of all interested parties (public authorities, consumers, users and industries) in the drafting, implementation, evaluation and control of the codes of conduct This participation is judged as necessary in order to legitimate the recourse to self-regulatory solutions.

The draft Proposal of a directive on certain legal aspects of the electronic commerce establishes in the same way, that as regards the code of conducts "in so far as the consumers may be concerned, the consumer associations shall be envolved in the drafting and implementation of these codes". Moreover, the actors must ensure their complete transparency and accessibility including as regards their evaluation.

*14. "Adequate" protection, or how a state authority can impose its values in a flexible manner on a third country in the global information society (Y. Poullet, B Havelange)* – By virtue of Article 25.1



of the directive, "the member States stipulate that, in the event a transfer to a third country of personal data as the object of a process, or intended to be subjected to a process after transmission, such a transfer may not take place unless, subject to national provisions taken in application of other provisions of the present directive, the third country in question can assure an adequate degree of protection". The principle is therefore to prohibit transmission unless an adequate level of protection can be proven by the third country.

The directive, rendering this yet more precise in Article 25.2, goes on to say that an evaluation of the adequate nature of data protection in a third country must take into account "all circumstances relating to a transfer or type of transfer" and in particular the different factors, of which some are integral to the type of transfer being considered, such as the nature of the data itself, the finality and the duration of the process, the country of origin and the country of destination, and others concerning the level of protection in the third country such as "current legal provisions both general and sectorial, as well as professional rules and the security measures which are respected there".

In particular, the text of Article 25 presumes a functional approach, that is to say, that the protection should be evaluated as much according to the risk of attack to the data's protection, risks arising from the type of flow in question, as according to the specific or general measures undertaken by the party responsible for the data in the third country to reduce such risks.

The evaluation of these measures should be made without a priori. There is no question here of imposing European mechanisms developed in response to the directive on a third country (no European imperialism), but rather of appreciating to what degree the goals of protection pursued by the directive are encountered there, whether in an original way or not. In this sense, the idea of adequate protection does not in any sense represent a weakening of that data protection envisaged by the directive. In effect, the idea of adequate protection induces a confrontation between the Data Protection fundamental requirements of the directive and the responses given to these by the third country. The aim is to see whether there is a "functional similarity". The "functional similarity" implies that we are concerned to find, not a pure and simple transposition of European principles and systems of protection in the third country, but rather the presence of those elements fulfilling the required functions, even if the said elements are of a different character to those we are familiar with here in Europe. This certainly encourages a better respect of the local structures and legal characteristics than would the

requirement of equivalent protection, which calls for a complete legislative similarity.

In particular, with regard to the regulatory instruments enacted in the third country, Article 25 does not only refer to norms established by public authority, whether general or sectorial in character, but equally to codes of conduct or technical measures, provided these are "respected". Thus the person entrusted with evaluating foreign protection would be more attentive to the "effectiveness" of an instrument than to its nature: what matters is that knowledge of the instrument in question, even if it is just a simple company privacy policy, be widespread among the persons concerned and among those responsible for files; similarly the trustee would be mindful of the option of claims or appeal by individuals calling those responsible to account in the event of any non-respect of these instruments. Finally, he would meticulously evaluate the quality of the authority in charge of claims and appeals, its accessibility and its functional transparence (Working Paper of the art. 29 Working Group, 1998).

*15. Regarding the conditions of self-regulation* – What conclusions can we draw from these two provisions of the "Data Protection" directive to serve as lessons both as to the value of private norms as well as to the synergy between these and the norms established by the state?

Firstly, the private norm is the better accepted for being defined within the framework of principles or standards established by the state norm. Such standards not only enable an evaluation of the private norm's conformity of content to society's expectations, but also assure it greater effectiveness.

Secondly, the private norm may be deemed "adequate" with regard to a state norm if the procedure under which it was drawn up conforms to certain demands of legitimacy: one, in the degree to which that procedure has permitted the expression of the opinions of, and taken into consideration the interests of, the different parties concerned by the operations to be regulated; and two, the transparency of the norm in questions more important is the question whether the private norm is genuinely effective, which is to say that binding sanctions can be pronounced by an authority equipped with powers of investigation, acting independantly of the parties concerned, easily accessible to all and whose dealings and advices are transparent (for example, via a public report of its activities, or the publishing of its decisions).



## Conclusions

*16. The state norm: a necessary intervention* – We must ask, with regard to state sources: what is the use of a national legislature legislating when, as we have shown, firstly, the international character of the network, and secondly, the impossibility of mastering the space-time co-ordinates of exchanges leads us to admit the impotence of nation states in the effective application of the norms they have drawn up? The emotion caused in 1996 by the intervention of a German court, charging access servers with having allowed pornographic material to filter through, shows however, that even if state law does not have completely effective instruments at its disposal, it is nonetheless capable of motivating private parties to put self-regulatory solutions in place which are at least partially if not totally satisfactory. The state, therefore, cannot simply resign, but rather, without pretending to police the network in a thorough manner, it should duly call attention to the social values that enshrine the norms, even if this is only in order to provoke appropriate self-regulatory reflexes and to serve as their basis. It is quite noticeable that even in U.S, country which is deemed to be the leader in the defense of the self-regulatory solutions, the public bodies are playing a greater and greater role in promoting even requesting these solutions. So, in Aug. 98, Mr Pitofsky, chairman of the Federal Trade Commission, has asserted: "Unless Industry can demonstrate that it is developed and implemented broad-based and effective self-regulatory programs by the end of this year, additional government authority would be appropriate and necessary". Since this asserting before the Congress, the american Government has take different initiatives like the "Global Alliance" in order to protect efficiently the privacy, in the context of its discussion with the European Union according to the request of article 25 of the Data Protection Directive.

Furthermore, the search within supra-national bodies like Unesco for common principles and solutions in areas such as the protection of minors, of consumers, of the signature etc., favourizes the normalizing of working channels, indeed co-operation (even if only among police forces!) between the states. In the absence of such a consensus, the position taken by a supra-national organization such as the European Union can serve as a departure point for international negotiation with other countries also entrusted with the search, doubtless via means more in keeping with their own legal traditions, for adequate protection vis-a-vis the principles enunciated by the European Union.

Confronted with the social revolution that the Internet represents, particularly the dislocation of space-time frontiers, state law, the expression of the social regulation of behaviour, is – and has a right to remain – present. The law cannot allow itself to be content with deploring the limitations placed on its own enforcement and affirming the essential lawlessness of cyberspace. On the contrary, it must find, in the context of a pluralist normative expression, an adequate active role. As far as possible it will refer, by application, adaptation or reform of general principles, to the normative mechanisms present in the network: the application of principles via self-regulation, technical standardization,... Depending on the case, it will draw its inspiration for the defining of rules of law, if possible at the international level, from the content of internal network regulation. What we are seeing here, to use M. Vivant's expression (Vivant, 1997), is without doubt the emergence of post modem law, or what J. Reidenberg (Reidenberg, 1996) refers to as a new "network governance paradigm".

Far from sanctioning the state's resignation, this "post modern law", this new "paradigm" calls for the creation of new forms of dialogue both between diverse ethical and regulatory normative techniques and, a more difficult task, between the democratic authorities capable of nurturing such a dialogue and placing it at the service of the public interest.

On the one band, the state cannot abandon Internet regulation to the sole initiative of its users. We have clearly seen that, in the absence of specific regulations, a reaffirmation of major legal principles spurs the parties to take measures and leads to the development of appropriate techniques.

On the other hand, we should like to stress the state's vital obligation to intervene at a time when, in our opinions deserting the Internet and withdrawing from the field of regulation to such a point that, if it no longer even decides the general framework, would notably put at risk public order, fundamental liberties and other basic values.

The precise division of labour between the drawing up of state or supra-national law and the regulatory initiatives of Internet users remains to be defined. It will doubtless be a dynamic relationship, and one which must enable the users to demonstrate a certain creativity in the enactment of the framework proposed by state legislation.

*17. The value and limitations of self-regulation* – This said, there can be no question of rejecting self-regulation as a normative source in the fullest sense of the term. As F. Osman (1995) concluded, "whether we choose to see in this uniquely «a question of time and



context» or the proof that the law must «progressively suffer both the attraction and the yoke of the economic facts» which dominate it and to which it has become a tributary", such a phenomenon can only serve to awaken the interest of lawyers who have been taught that the sanction is part of the mechanism of the rule of law. It naturally arises that they are tempted to search everywhere, even in "soft" law. And if the criteria of the sanction as a "characteristic of the rule of law is a false criteria, despite doctrinal attempts to revive it, this is doubtless because the effectiveness of rules of social conduct, whether they "rule or regulate", does not necessarily reside in the adherence to them by the social body for which they are destined".

This reflection, which addresses the normative sources of "lex mercatoria" ought to be equally applicable to "lex electronica", certainly, but it cannot have the same range and, without a doubt, this justifies a more resolute intervention on the part of state law. Firstly, the internaut environment, except in the News group context, or in certain situations such as universities or trade between merchants, does not have anything like the same homogeneity as that of professionals. Secondly, where "lex mercatoria" only regulates economic questions, "lex electronica" is concerned with culture, values and liberties.

It would appear from this, therefore, that self-regulation should be controlled. 'Rough it is certainly capable of representing the spontaneous expression of a particular community, this is rarely the case. Furthermore, state law is obliged at least to fix the standards which serve as a basis for the development of self-regulation and its associated normative techniques and to see to it that the mechanisms for the setting up of these regulatory techniques and the application of the content of these private norms is transparent and takes into account the interests of the various parties concerned.

**Bibliografia**

La bibliografia è consultabile al sito:
www.droit.fundp.ac.be/textes/droit-du-cyberspace.pdf